Translation

PATENT COOPERATION TREATY

PCT

PCT/IB2003/004190

528787

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P-14-425-PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/IB2003/004190	International filing date (*day/month/year*) 19 septembre 2003 (19.09.2003)	Priority date (*day/month/year*) 24 septembre 2002 (24.09.2002)
International Patent Classification (IPC) or national classification and IPC H04N 7/16		
Applicant NAGRACARD SA		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
13 April 2004 (13.04.2004)	29 December 2004 (29.12.2004)
Name and mailing address of the IPEA/EP D-80298 Munich Tel. +49 89 2399-0 Facsimile No. +49 89 2399-4465	Authorized officer Fassnacht, C Telephone No. +49 89 2399-6019

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/IB2003/004190

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☒ the international application as originally filed.

☒ the description, pages 1-9, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1-9, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/1, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/IB 03/04190

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-9	YES
	Claims		NO
Inventive step (IS)	Claims	1-9	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-9	YES
	Claims		NO

2. Citations and explanations

The invention concerns a multiple matching control method.

This report makes reference to the following document:

D1: WO 00/59222 A (SONY ELECTRONICS INC), 5 October 2000 (2000-10-05)

Document D1 is considered to constitute the prior art closest to the subject matter of claim 1 and discloses (the references in parentheses are to that document) a method for checking a match between a removable security module ("smart card") and a host appliance ("host"), the match being used to secure a data exchange by means of a single match ("Unique Key"; see page 10, lines 25 to 28).

The subject matter of claim 1 differs from that method in that the claimed method involves the initiation of a matching process using a secret key common to multiple devices (such as multiple removable security modules) to encrypt a cryptogram, which is then decrypted by a first device (such as one of the multiple removable security modules) in order to extract therefrom the identifier of a second device (such as a host appliance) and to generate a matching key based on the identifier and which will be

stored in the first device. This method solves the problem of performing the match without the need for a management centre to authorise the match, in particular in an environment in which a management centre cannot be contacted during the match or when no link exists between the management centre and the security module.

This use of a secret key common to multiple devices to generate a matching key is not disclosed or suggested by document D1 or by any other document cited in the search report.

Claim 1 thus meets the requirements of PCT Article 33. Claims 2 to 9 are dependent on claim 1 and thus also meet the PCT novelty and inventive step requirements.

Box VII

Certain defects in the international application

Contrary to PCT Rule 5.1(a)(ii), the description does not cite document D1 or indicate the relevant prior art disclosed therein.

Box VIII

Certain observations on the international application

The single independent claim 1 does not meet the requirements of PCT Article 6 for clarity for the following reasons:

- the phrase "all the first devices" is unclear because claim 1 referred up to that point only to "a first device" in the singular, and specified "such as a removable security module"; it does not define a plurality of first devices (by contrast with "the second device, such as a host appliance").